SECRET

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, D.C. 20330

16 JUL 1968

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY WORKING GROUP

SUBJECT: Computer Security Problem Areas - Air Force (U)

1. Attached is a list of eight problem areas which, at the present time, have been identified within the Air Force.

2. Except for the first listed problem, no attempt has been made to address priority since no one item was stressed more than any other.

3. To some degree, all identified problem areas are experienced in Air Force organizations worldwide.

4. Apropos of the task to identify security problem areas involving ADP, are the questions: "Is this really a security problem?" and if so, "How serious is the problem?" Relevant comments in this regard appear with some of the identified problems.

Hays Bricka

HAYS BRICKA, Lt Colonel, USAF
Air Force Representative
Computer Security Working Group

1 Atch
List of Computer
Security Problem
Areas, (S)

Copy to: CIA
D/State
AEC
FBI
DIA
Army
Navy

USAF review completed.

SECRET

Upon removal of Atch(s) this correspondence becomes UNCLASSIFIED.

COMPUTER SECURITY PROBLEM AREAS - AIR FORCE

1. The requirement to sanitize computer tapes, disks, disk packs and drums.

COMMENT: Degausssing works well for tapes containing non-compartmented information. Because of relatively low cost, physical destruction of tapes containing compartmented information is feasible. However, this situation does not apply to the sanitization of disks, disk packs and drums when compartmented information is involved. In these cases destruction of the disks, disk pack or drum seems to be the only, and very costly, answer since degaussing and overprinting is apparently not recognized as being adequate.

2. The integrity of individual files and executive programs.

COMMENT: It is believed that protection of individual files and executive programs must be made apart of the software through use of special key words, lock-outs, etc. At present it has been accomplished to a limited degree by writing in legal and illegal queries or actions. This technique can become inordinately complicated, time consuming and wasteful of storage space.

3. The requirement to sanitize internal memory cells.

COMMENT: It is felt that there are times when this would be necessary - e.g., when highly classified and/or compartmented material was being run and a breakdown calling for customer engineer services would be required, or upon completion of a classified job on a computer normally used for unclassified work.

While this is a security problem, it is believed that solution should and could be relatively simple. Possibly no more than turning the power switch off and then on again would be required.

4. The requirement for physical security of the ADP equipment/ installation and personal security clearances and access authorizations for the facility's personnel.

COMMENT: Here we are faced with several real or imagined problems. The elementary steps are obviously taken care of

by restricted areas, locks, guards, and other authorized access controls. However, other steps may be necessary such as shielding against RF emissions and feed back through power lines. Also, in overseas locations, rules concerning the hiring of indigenous personnel must be developed or considered.

It is recognized that computer emissions are a reality. However, are these emissions really a security problem? How serious is this problem? (By hearsay, the IBM 360 generation computer can be intercepted for a considerable distance. However, it has been said that it would take an identical IBM 360 computer 10 years to translate the intercepted data into intelligible information.) This area should be explored and clarified. We need answers to the questions: Are computer emissions a security problem? How much of a problem? Will shielding really work? Is the risk worth the cost of shielding?

5. The requirement to prevent the inadvertent "dump" of information.

COMMENT: In the past, this has not been a particular problem, but with the introduction of third generation computers and remote query devices capable of simultaneous operation this is now a problem. Here the problems of "need to know" and inadvertent disclosure become the greatest. Inadvertent "dump" through design or accident is both possible and probable regardless of the safeguards created in the software portion of the system. We don't even pretend to have an answer for this problem.

6. The requirement for computer communications security.

COMMENT: This problem involves both the security of communications between computers, and between computers and remote query devices. Encryption devices, line shielding and the use of special key words, codes, lock-outs, etc., may provide the solution.

7. The problem of contracting for computer services and associated functions.

COMMENT: The increase in workload beyond the design or facility's capability may cause an organization to contract for the performance of the excess work. Equipment breakdown may also bring this situation about. The contractor may be private industry, a non-USIB U.S. government agency, or a USIB agency. Security standards and procedures are now non-standard and in some respects non-enforceable.

8. The possibility of colocating Command and Control and IDHS ADP.

COMMENT: The JCS are considering the preparation of policy guidance on the colocation* of Command and Control** and IDHS*** ADP facilities. Should this materialize and colocation as addressed become a reality it would not necessarily mean joint use of a single computer. However, future installations would almost surely be required to use the same equipment. Such situations would impinge on all aspects of computer security and personal security forcing the entire facility to be up-graded from the overall security point of view.

Here again we are dealing with the problems of "need to know", inadvertent disclosure, and inadvertent "dump" of information because we are dealing with all security classifications and access authorizations in the same place and often at the same time.

*Colocation - (JCS) The positioning of two or more ADP facilities within one computer center.

**Command and Control - (JCS) An arrangement of personnel, facilities, and the means for information acquisition, processing, and dissemination employed by a commander in planning, directing and controlling operations.

***Intelligence Data Handling System - (AF) Information systems for the processing and manipulation of intelligence data for the operational purposes of military intelligence organizations and agencies. They are characterized by the application of general purpose computers, peripheral equipment, and automated storage and retrieval equipment for documents and photographs.